REMARKS

Priority

A priority claim under 35 U.S.C. 119 and a certified copy of the priority document are submitted concurrently herewith.

Objections

The Examiner objected to claims 12, 16, 20, 21, 24, and 28 as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicants note that claim 21 is an independent claim and that dependent claim 32 incorporates some of the features of the claims to which objection was made. Applicants have therefore amended claims 12, 16, 20, 24, 28, and 32 to recite "performing the modulo operation if computation of a discrete logarithm is not possible." Applicants respectfully submit that the respective parent claims do not recite performing a first computation if a second computation is not possible and that these dependent claims as amended therefore further limit the parent claims.

35 USC 112

Claims 9-12, 17-19, 25-28, and 32 stand rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement. The Examiner stated that the specification does not describe "encrypting the plurality of encryption keys using a first key." Applicants have amended independent claims 9, 13, 17, 21, 25, and 29 to clarify that the encryption is performed using a "cryptography scheme" instead of a "key."

Applicants submit that this amendment is supported by the specification at least at page 4, lines 21-25, wherein it is described that "the keys (512) remain encrypted with the user's encryption scheme...Once the user (102) receives the keys (512) back from the database (104), the next step is simply to decrypt them using the user's own decryption scheme (604), thus revealing the unencrypted keys (204)."

Claims 9-32 stand rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. Applicants have amended independent claims 9, 13, 17, 21, 25, and 29 to more

clearly describe the invention and respectfully submit that the amendments overcome the rejection.

35 USC 102(b)

The Examiner rejected claims 9-32 under 35 USC 102(b) as unpatentable over Gammie. This rejection is respectfully traversed.

Applicants submit that Gammie fails to disclose the claimed invention. Gammie describes a system in which content is doubly encrypted before transmission to a receiver. Gammie, in the Summary, describes that "the present invention...twice-encrypts the key prior to transmission, first with a first secret serial number (SSN_1) of the subscriber's replaceable security module, and again with a second secret serial number (SSN_0) of the subscriber's decoder...The system further comprises a transmitter coupled to the signal scrambler and the second key encryptor for transmitting the scrambled signal and twice-encrypted key."

According to Gammie, the twice-encrypted content is received at a receiver where it is twice-decrypted. Gammie describes that "[t]he first key decryptor is coupled to the transmitter and performs a first key decryption on the twice-encrypted key using the second secret serial number and outputs a partially decrypted key. The second key decryptor is coupled to the first key decryptor and perform a second key decryption on the partially decrypted key using the first secret serial number and outputs the decrypted key."

In contrast, the pending claims describe that a once-encrypted key is transmitted from a database to a requester. At the requester, this key is then encrypted a second time and sent back to the database as a twice-encrypted key. At the database, the key is once-decrypted and sent back to the requester. At the requester, the key is completely decrypted and used to decrypt a digital object.

Gammie only describes a simple one-way system whereby content is doubly encrypted at a transmitter and then doubly decrypted at the receiver. The claimed invention, however, enables a user to securely request content from a database while obscuring from the database

operator what content was of primary interest to the requester. Gammie completely fails to describe a system capable of this operation.

In view of the above, each of the presently pending claims in this application is in immediate condition for allowance.

In the event the U.S. Patent and Trademark Office determines that an extension and/or other relief is required, applicants petition for any required relief including extensions of time and authorize the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 03-1952 referencing docket no. 455392000900.

Dated: April 18, 2006

Respectfully submitted,

By _____

James M. Denaro
Registration No.: 54,063
MORRISON & FOERSTER LLP
1650 Tysons Blvd, Suite 300
McLean, Virginia 22102
(703) 760-7739